Quelques réflexions à propos de la délibération n°19/2008 du 7 mai 2008 émanant du comité sectoriel registre national

Poullet, Yves

Published in:
Revue du Droit des Technologies de l'information

Publication date:
2008

ACTUALITÉ

Quelques réflexions à propos de la délibération n° 19/2008 du 7 mai 2008 émanant du comité sectoriel registre national[1]

Yves Poullet[2]

La délibération dont question répond à la demande du Service public fédéral (en abrégé : S.P.F.) Fedict d'accéder aux informations du registre national et d'utiliser le numéro d'identification de ce registre en vue de tester, corriger et entretenir des applications informatiques qui ont une connexion avec le registre national via l'U.M.E., le F.S.B. et les webservices.

Elle est prise sur la base d'un avis technique et juridique émanant du registre national dont la teneur est largement négative et auquel la délibération du comité sectoriel ne répond en aucune manière.

La délibération autorise Fedict « à accéder en permanence à toutes les informations du registre national tant aux informations de base qu'aux informations de l'historique et à utiliser le numéro de registre national sous quelques conditions : détermination par le conseiller en sécurité de la population « test » qui ne peut excéder un maximum de 10 000 personnes et contrôle par ce même conseiller en sécurité du respect des conditions que lui-même émet.

En outre, la délibération dispense le personnel et les sous-traitants de Fedict de toute obligation de s'authentifier personnellement. Lors de l'accès au registre national, Fedict peut se contenter d'un certificat d'application. Quant à ses obligations de sécurité, la délibération prévoit que le S.P.F. devra répondre à un questionnaire que le comité sectoriel lui adressera, le cas échéant, en matière de sécurité de l'information.

La délibération en question soulève diverses interrogations. À tout le moins, on en relève quatre.

1. La demande de Fedict s'inscrit dans la ligne de précédentes demandes d'autorisation déjà introduites avec succès par ce Service public fédéral. Il s'agit pour Fedict de développer des services nouveaux au profit des citoyens, fonctionnaires ou autres autorités publiques. Ainsi, la délibération n° 26/2005 permet à Fedict de gérer les moyens d'identification et d'authentification électroniques des utilisateurs de services électroniques, en vérifiant auprès du registre national et, le cas échéant, d'autres sources, la qualité et l'identité des demandeurs d'accès aux services ou bases de données publics, accessibles par voie électronique, que ces demandeurs

[1] Nous remercions E. Degrave pour sa relecture.

[2] Professeur ordinaire à la faculté de droit de Namur, directeur du C.R.I.D. – F.U.N.D.P., Yves.poullet@fundp.ac.be.

soient citoyens ou fonctionnaires. Celles du 25 mai 2005 (délibération n° 20/2005) et du 6 septembre 2006 (délibération n° 25/2006) autorisaient déjà Fedict à mettre en place un système sûr de communication via Internet pour les mineurs. Dans le même sens, la présente demande vise, au-delà de la demande d'autorisation de procéder à des opérations de test à propos des communications entre le registre national et les administrations, à permettre à Fedict de jouer un rôle de plate-forme de communication entre les administrations publiques existantes qu'elles soient fédérales, régionales ou communautaires et le registre national. Dans ce cadre, la demande entend autoriser Fedict à pouvoir tester la communication entre ces entités et le registre national. Des documents en provenance notamment de la Banque-carrefour de sécurité sociale indiquent la volonté de faire jouer à Fedict, dans le futur du moins, un rôle semblable à celui de la B.C.S.S. Face à cette volonté de Fedict de développer un rôle nouveau, il s'agit de s'interroger sur la possibilité de créer par de simples autorisations du comité sectoriel, en l'occurrence celui du registre national, de nouveaux traitements et d'accorder à Fedict une nouvelle compétence *ultra legem*. On rappelle à cet égard que l'article 22 de la Constitution exige que la création de traitements qui constituent une limite à la vie privée des citoyens fasse l'objet d'une loi au sens formel ou strict du terme.

2. À y regarder de plus près, l'objet de la demande est d'autoriser Fedict à compléter voire à se substituer au registre national pour effectuer le *testing* des communications autorisées (accès, transfert via ou non l'utilisation du numéro de registre national). Il est permis de se demander si ce faisant, le rôle de Fedict n'est pas à rapprocher de celui d'un sous-traitant offrant un système de transport plus sécurisé que celui d'un responsable de traitement.

3. La finalité des opérations menées par Fedict, objet de l'examen du comité sectoriel en question, est, selon la demande du Service public fédéral, le *testing* des communications que Fedict va gérer entre des personnes autorisées à accéder au registre national et ce dernier. Il n'est pas évident que le *testing* puisse en tant que tel être une finalité. C'est dans le cadre de connexions pour lesquelles Fedict peut jouer un rôle de transporteur que ces tests doivent opérés. En d'autres termes, le *testing* est une opération accessoire nécessaire à l'accomplissement d'une finalité : la bonne qualité et la sécurité d'un transfert dont la légitimité doit être vérifiée. C'est également à l'aune de la légitimité de ce transfert, que la proportionnalité des données testées doit s'apprécier. Ainsi, s'il s'agit de tester la qualité de la communication entre le registre national et une base de données des étudiants universitaires des Communautés de notre pays, on imagine mal que le test porte sur des données relatives à l'historique des parents de ces étudiants ou à leur adresse. En d'autres termes, on a quelques difficultés à comprendre que le *testing* puisse justifier un accès permanent à l'ensemble des informations du registre national. Les quelques limites (détermination de la population test sans lien avec la finalité de la communication et de l'autorisation d'accès justifiant l'intervention de Fedict et un maximum de 10 000 personnes) mises par le comité sectoriel apparaissent dérisoires au regard des exigences qu'impose l'article 4, § 1er, 3°, de la loi du 8 décembre 1992.

4. La décision d'autorisation substitue à l'obligation d'une identification individuelle des accès au registre national, une simple identification de l'application Fedict, qui peut être générée tant par des agents du S.P.F. que par des sous-traitants dont on ignore la qualité et les liens qui les unissent à Fedict. Cette substitution ne manque pas d'inquiéter du point de vue de la sécurité de l'accès au registre national

et, en tout cas, a pour conséquence d'empêcher le registre national d'exécuter l'obligation de sécurité que la loi de 1992 lui impose. Comment le registre peut-il vérifier que l'accès opéré sur la base de l'application Fedict soit légitime ? En outre, cette solution a pour effet de nuire à la transparence que le registre national doit aux citoyens lorsque ceux-ci souhaitent exercer leur droit d'accès. On sait que, pour le registre national, l'obligation de transparence a une portée particulière dans la mesure où la personne concernée doit pouvoir, par un moyen aisé, connaître le nom des personnes qui ont eu accès à ses données et être informée des corrections ou suppressions des informations qu'elle a pu leur communiquer. De telles mesures légales d'amélioration de la transparence sont mises à mal lorsque le log d'entrée et de sortie des données du registre national ne peut que mentionner le nom d'une application et non plus le nom des personnes ayant eu accès au registre national.

ANALYSE DES QUATRE ARGUMENTS

A. Fedict dispose-t-il d'une légitimité pour traiter des données à caractère personnel ?

La délibération du comité sectoriel tire argument des compétences de Fedict pour justifier la légitimité de sa demande. « L'article 2, § 1er, de l'arrêté royal du 11 mai 2001 portant création du Service public fédéral technologies de l'information et de la communication énumère les missions du demandeur... ». Les délibérations du comité sectoriel précédentes relatives à des traitements effectués par Fedict, celles du 25 mai 2005 (délibération n° 20/2005) et du 6 septembre 2006 (délibération n° 25/2006), se référaient également à ce texte fondateur du S.P.F.

Deux éléments nous amènent à nous interroger sur la légitimité de la demande de Fedict.

1. Les missions réglementaires de Fedict ne paraissent pas justifier une compétence nouvelle, celle d'intégrateur de services

La première concerne la difficulté de tirer des missions de Fedict telles que décrites dans cet arrêté royal la mission d'opérer des traitements qui, on le pressent, ne sont pas seulement des traitements ponctuels mais ont pour conséquence de faire de Fedict à l'instar de la B.C.S.S. un véritable « intégrateur de services ». Par cette notion, on entend une plate-forme gérant des flux nombreux au sein d'un secteur ou plusieurs secteurs administratifs et disposant à cette fin de bases de données de référence. Plusieurs présentations récentes attestent de cette volonté administrative sinon gouvernementale, qui n'est pas en soi condamnable si du moins sa réalisation respecte les règles de droit.

Or, à ce stade, l'arrêté royal de fondation de Fedict envisage celui-ci non comme un opérateur de traitements mais comme un service chargé de fonctions plus conceptuelles et non opérationnelles, comme l'aide, le conseil, la définition de protocoles ou d'applications, utiles pour les administrations en général ou particulières. Fedict, par ailleurs, élabore la stratégie qui doit faire de la Belgique le pionnier en matière d'e-gouvernement. Dans le cadre de la définition de cette stratégie, le site de Fedict énumère, à la suite de l'arrêté royal du 11 mai 2001 qui le crée, ses tâches principales comme suit :

« – encadrer les Services publics fédéraux qui exécutent cette stratégie ;
– développer les normes, standards et l'architecture de base ... à l'appui de cette stratégie ;
– développer des projets et des services ... qui soutiennent cette stratégie commune ;
– collaborer étroitement avec les partenaires des autres niveaux de l'administration (Europe, Communautés, Régions, provinces) ».

Bref, il est loin d'être évident que le Roi ait entendu confier à Fedict des tâches opérationnelles de gestion des infrastructures et des applications que, le cas échéant, elles développent. Sans doute, on objectera que le développement d'infrastructures modernes de communication, le Fedman, reposant sur le Fedbus et la mise sur pied d'un portail administratif commun comme le Fedweb impliquent des traitements y compris de données nominatives mais rien n'obligeait Fedict à en devenir responsable.

Or, la description des mesures de sécurité prises par Fedict dans le cadre du déploiement des protocoles U.M.E. et du F.S.B., description que le comité sectoriel approuve (point C2), laisse clairement entendre que Fedict jouera ce rôle dans l'avenir. Une telle modification ou plutôt un tel complément aux tâches de Fedict obligeait pour le moins à l'adoption d'un texte réglementaire voire législatif (*cfr infra)*, le chargeant explicitement de telles missions. La demande d'autorisation de Fedict relative au registre national dissimule donc mal le véritable débat : la transformation progressive de Fedict en une plate-forme sécurisée offrant des services similaires à ceux actuellement offerts par la B.C.S.S. dans le cadre de la sécurité sociale.

Une délibération du comité sectoriel de l'autorité fédérale[1] va dans ce sens et pointe la nécessité de cette intervention au moins réglementaire. « La Commission estime qu'à la lumière de ce qui précède, il est recommandé de prendre des dispositions de manière à permettre non seulement l'accès aux données reprises dans ces banques de données ou leur communication, mais aussi la réalisation d'associations avec celles-ci afin que notamment l'article 4 de la loi vie privée soit respecté de manière optimale. Cela implique l'intervention d'un tiers de confiance, par analogie avec le rôle assuré par la Banque-carrefour de la sécurité sociale... Il semble recommandé que Fedict assure un tel rôle en ce qui concerne les données qui relèvent de la compétence du comité sectoriel pour l'autorité fédérale. La Commission insiste dès lors pour que Fedict prenne les dispositions nécessaires à cet effet le plus rapidement possible ». Si tel est le but à moyen terme de Fedict, il eût été utile que la demande de lui voir reconnaître un rôle plus opérationnel de véritable responsable de traitement soit formulée de manière explicite et surtout que ce rôle de « Trusted Third Party » trouve son fondement dans un texte réglementaire voire une loi.

2. *Cette compétence nouvelle devrait avoir une base légale*[2]

À cet égard, précisément, l'article 22 de la Constitution n'exige-t-il pas que de telles compétences nouvelles soient attribuées dans le cadre d'une loi au sens strict du terme et non d'un simple arrêté royal ? L'article 22 de la Constitution belge[3] traduit[4] dans notre ordre juridique le principe de l'article 8 : « Chacun a

[1] Délibération 05/2007, point 32 où le comité souhaite conférer à Fedict un rôle similaire à celui de la B.C.S.S.

[2] Sur ce point, nous nous référons aux réflexions publiées *in* D. De Roy, C. de Terwangne et Y. Poullet, « La Convention européenne des droits de l'homme en filigrane de l'administration électronique », *C.D.P.K.*, 2007, 2, p. 328.

[3] L'article 22 de la Constitution dispose que « Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit ». Cette disposition (anciennement l'article 24*quater*) a été introduite par la modification à la Constitution du 31 janvier 1994 (*M.B.*, 12 février 1994, p. 3670).

[4] « Il ressort des travaux préparatoires de l'article 22 de la Constitution que le constituant a cherché la plus grande concordance possible avec l'article 8 de la Convention européenne des droits de l'homme afin d'éviter toute contestation sur les contenus respectifs de l'article de la Constitution et de l'article 8 de la Convention (*Doc. parl.*, Chambre, sess. 1993-1994, n° 997/5, p. 2) » (C.A., arrêt 16/2005, 19 janvier 2005).

droit au respect de la vie privée et familiale, sauf dans le cas et conditions fixés par la loi ». Cette traduction belge des exigences européennes comporte cependant une précision importante. Alors que l'exception prévue par la Convention européenne s'entend d'une loi au sens matériel, l'exception belge s'entend de la *loi au sens formel*, c'est-à-dire de l'acte réglementaire pris par un pouvoir législatif peu importe le niveau où il s'exprime. Ainsi le rappellent le Conseil d'État[5], la Cour d'arbitrage devenue Cour constitutionnelle[6] sans oublier la Commission de la protection de la vie privée[7].

Ainsi, comme le note la Cour d'arbitrage, dans l'arrêt n° 202/2004, « l'exigence d'une loi au sens formel s'impose en Belgique pour autoriser une ingérence dans ces droits, en vertu de l'article 53 de la Convention. Cet article prévoit que lorsqu'un droit ou une liberté est davantage protégé par les dispositions nationales que par la Convention, c'est à ces dispositions nationales qu'il convient d'avoir égard ». L'affirmation est répétée dans l'arrêt n° 131/2005 du 19 juillet 2005 : « Bien que l'article 8.2. de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une « loi » au sens formel du terme, le même mot utilisé à l'article 22 de la Constitution désigne une disposition législative »[8]. Notre propos est simplement de rappeler à Fedict cette contrainte légale voulue expressément par notre législateur. La base légale qui permettrait à Fedict d'être lui-même responsable de traitement manque en droit belge et il est difficile de tirer d'un texte de simple valeur réglementaire dont la portée est loin d'être précise la base légale de tels traitements. La même remarque peut être adressée à la délibération n° 26/2005 du 6 juillet 2005 qui tire des articles 133 et 134 de la loi-programme du 8 avril 2003, qui fixe le mode par lequel les citoyens pourront s'identifier et s'authentifier électroniquement vis-à-vis des administrations, la compétence de Fedict, d'abord, de se connecter au registre national et d'utiliser le numéro d'identification du registre national, ensuite, de traiter et conserver ces données d'identification et d'authentification.

En conclusion, il nous semble que la loi aurait dû prévoir l'existence de ce traitement, nommer Fedict responsable de ce traitement comme le prescrit l'article 1er, § 4, de la loi du 8 décembre 1992[9] et fixer les conditions minimales de ce

5 Avis du Conseil d'État relatif au projet de loi organique des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 1995-1996, n° 638/1, p. 31 : « L'article 22 de la Constitution impose en particulier au législateur fédéral l'obligation de garantir la protection du droit au respect de la vie privée et familiale : il est, à l'inverse, seul habilité à déterminer les cas et les conditions dans lesquels ce droit peut souffrir certaine restriction ». Sur d'autres avis du Conseil d'État, en particulier, ceux rejetant la possibilité de limiter la vie privée par des arrêtés royaux même de pouvoirs spéciaux voire par des lois-programmes, voy. la liste et les commentaires de J. Velaers, « De Grondwet en de Raad van State, afdeling Wetgeving », *in De Grondwet en de Raad van State, afdeling wetgeving, vijftig jaar adviezen aan wetgevende vergaderingen in het licht van de rechtspraak van het Arbitragehof,* Anvers, Maklu, 1999, p. 154.

6 *Cfr* C.A., arrêt n° 202/2004 relatif à la loi du 6 janvier 2003 concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête : « L'article 8.2. de la convention précitée qui permet une ingérence d'une autorité publique dans les droits qu'il garantit n'exige pas que cette ingérence soit prévue par une "loi" au sens formel du terme, le mot « loi » y signifiant toute règle de droit d'application générale et impersonnelle. Par contre, le même mot « loi » utilisé à l'article 22 de la Constitution désigne une disposition législative ».

7 Ainsi, dans son avis récent à propos des listes noires (avis n° du 15 juin 2005), la Commission affirme : « La Commission a déjà rappelé dans son avis « Phénix » susmentionné que « on sait que le Conseil d' État s'est déjà opposé à la création de traitements par simple arrêté royal et exige que les éléments essentiels des traitements du secteur public (finalités, types de données traitées) soient fixés par la loi elle-même ».

8 C.A., arrêt n° 131/2005 du 19 juillet 2005, marginal B.5.1.

9 « Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu d'une loi, décret

traitement comme le prescrit l'arrêt *Rotaru* de la Cour européenne des droits de l'homme[10]. L'affaire *Rotaru* relative à l'enregistrement du passé d'un citoyen roumain par des services de renseignements précise indirectement le contenu minimal d'une loi créatrice d'un traitement de données personnelles, pour satisfaire aux exigences de prévisibilité : « Or, dit l'arrêt, aucune disposition de droit interne ne fixe les limites à respecter dans l'exercice de ces prérogatives. Ainsi, la loi précitée ne définit ni le genre d'informations pouvant être consignées, ni les catégories de personnes susceptibles de faire l'objet de mesures de surveillance telles que la collecte et la conservation des données, ni les circonstances dans lesquelles peuvent être prises ces mesures, ni la procédure à suivre. De même, la loi ne fixe pas de limite quant à l'ancienneté des informations détenues et la durée de leur conservation ».

Il m'apparaît donc contraire à l'esprit et à la lettre de l'article 22 de la Constitution que la création d'un traitement puisse être confiée à une autorité n'ayant pas reçu compétence légale pour ce faire et que c'était à la loi de fixer les éléments essentiels des traitements confiés à Fedict. Comme le rappelle la Commission de protection de la vie privée dans l'avis tout récent[11] qu'elle a prononcé à propos de la création de la source authentique des données relatives aux véhicules, « Le principe de légalité découle de la loi sur la vie privée et de l'article 22 de la Constitution... Essentiellement seul le législateur est donc compétent pour établir un système général qui vise à collecter des données à caractère personnel à grande échelle, à les traiter et à les transmettre pour diverses finalités incluant la participation d'un grand nombre de services publics et d'organismes privés. La Commission doit vérifier si les éléments essentiels sont réglés de manière suffisamment précise dans l'avant-projet... »[12]. Si la doctrine de la Commission mère sur ce point apparaît claire, comment expliquer que le comité, fille de cette dernière, ignore à ce point l'enseignement maternel ?

L'interrogation se prolonge si on s'interroge sur la nature de l'intervention de Fedict. N'est-il pas sous-traitant plutôt que responsable de traitement ?

B. Fedict apparaît en définitive plus comme un sous-traitant que comme un responsable de traitement lorsqu'il demande l'accès au registre national

La délibération en question justifie le traitement comme suit : « Le demandeur a développé l'U.M.E., le F.S.B. et/ou les webservices au profit des autorités fédérales. L'élaboration de telles applications ne constitue pas en soi une garantie d'un service de qualité. Ce n'est qu'après des tests concluants... qu'une application peut être mise en production. Il faut ensuite assurer l'entretien de l'application. Tout ce processus, essentiel au développement de projets d'e-government, s'inscrit dans le cadre des missions réglementaires du demandeur (soit de Fedict) ». La délibération poursuit : « Certaines applications informatiques ont accès à des sources authentiques telles que le registre national, via l'U.M.E., le F.S.B. et les webservices, pour autant que les instances qui utilisent ces applications disposent des autorisations requises du comité sectoriel compétent ».

ou ordonnance, le responsable du traitement est la personne physique, la personne morale, l'association de fait ou l'administration publique désignée comme responsable du traitement par ou en vertu de cette loi, de ce décret ou de cette ordonnance ».

10 C.E.D.H.., arrêt *Rotaru c. Roumanie* du 4 mai 2000, req. 28341/95, § 57, publiée *in Rev. trim. dr. h.*, 2001, pp. 137 et s., note O. De Schutter.

11 Disponible sur le site de la Commission (http://www.privacycommission.be).

12 L'avis propose même une méthodologie de rédaction pour la définition des éléments essentiels.

De cette double assertion que peut-on tirer ? Fedict, et c'est bien son métier comme nous l'affirmions au point 1, a pour mission de développer des applications (U.M.E., F.S.B. ...) dont l'utilisation peut être générique ou commune à plusieurs administrations. Dans le cadre de ces développements, elle peut être confrontée à des demandes venant de certains utilisateurs, de se connecter à des sources authentiques et en particulier au registre national. Dans ce contexte, Fedict agit alors comme un sous-traitant et ne dispose pas d'autre droit d'accès au registre national que celui pour lequel il est mandaté par l'autorité qui le lui demande.

La loi du 8 décembre 1992 distingue en effet deux qualifications possibles pour celui qui traite des données à caractère personnel. Il s'agit de le qualifier soit de responsable du traitement, soit de sous-traitant. La distinction suit le critère de la finalité et des moyens. Le responsable du traitement est celui qui détermine, précise l'article 1er, § 4, de la loi vie privée, « les finalités et les moyens du traitement des données à caractère personnel ». Le sous-traitant, par contre, agit dans l'ombre du responsable du traitement, car, selon l'article 1er, § 5, de la loi, il « traite des données à caractère personnel pour le compte du responsable du traitement et est autre que la personne qui, placée sous l'autorité directe du responsable du traitement, est habilitée à traiter les données ».

Selon la loi, le responsable de traitement est la personne qui détermine les finalités et les moyens du traitement de données à caractère personnel. Si les finalités et les moyens sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le responsable de traitement est la personne désignée comme telle par ou en vertu de cette norme de valeur législative[13]. En l'occurrence, l'accès au registre national poursuit une finalité qui est définie et vérifiée par le comité sectoriel *ad hoc* dans le chef de l'autorité administrative qui par ailleurs décide pour ce faire d'utiliser les moyens mis à sa disposition pour Fedict et non pas dans le chef de ce dernier.

Que les multiples demandes d'accès au registre national via les interfaces proposées par Fedict justifient une certaine forme de mutualisation du service offert par Fedict peut se concevoir mais il n'en reste pas moins que celui-ci lorsqu'il « teste » les connexions de chacun de ses « clients » via les connexions qu'il opère, le fait à la demande et sur la base des autorisations obtenues par chacun d'eux. Cette qualification de sous-traitant de Fedict a une conséquence. Récemment, à propos de « L'externalisation de l'administration, les nouvelles technologies et la protection de la vie privée[14] », Mme Degrave et moi-même écrivions : « Au-delà, l'article 16, § 1er, de la loi exige la signature, en marge de l'adjudication, d'un contrat par lequel les mesures de sécurité retenues seront dûment respectées et qui rappellera à l'adjudicataire qu'il « n'agit que sur la seule instruction du responsable du traitement ». Le contrat peut être écrit ou sur support électronique. La similitude de l'hypothèse que nous visions et celle visée par la demande de Fedict nous apparaît évidente : « Finalement, signalons que si plusieurs administrations recourent à un même sous-traitant, chacune d'entre elles reste responsable des traitements particuliers qu'elle confie à ce dernier. Il ne peut être question de désigner un seul responsable, dans la mesure où les finalités poursuivies par chacune des administrations sont bien distinctes. Il est dès lors nécessaire

13 Article 1er, § 4, de la loi vie privée.

14 Article paru au *J.T.*, 26 avril 2008, pp. 277 et s. Cet article concernait les relations entre une administration soit concessionnaire d'un service public soit adjudicataire d'un marché public et une entreprise privée mais le raisonnement y tenu peut également s'appliquer aux hypothèses où une administration agit au nom et pour le compte d'une autre administration.

que des mesures soient prévues avec le sous-traitant pour qu'un cloisonnement réel entre les données en provenance de ces différentes administrations soit assuré tant sur le plan technique qu'organisationnel »[15]. Cette assertion a des implications importantes en ce qui concerne la sécurité des opérations effectuées par Fedict auprès du registre national comme nous le montrerons au point 4.

La demande de connexion de Fedict ne peut se concevoir en effet que comme une sous-traitance. S'il s'agit de « tester » des connexions entre des administrations et le registre national, ce ne peut être qu'au regard des traitements qui sont autorisés dans le chef de chaque administration et pour ses seuls besoins. Pour répondre à cette objection, Fedict se justifie en parlant d'une finalité générale de *testing*, qui dans la mesure où nombre d'administrations peuvent souhaiter se connecter ou sont obligées d'utiliser les applications de connexions développées par Fedict légitimeraient dans le chef de Fedict une demande propre d'autorisation de connexion. C'est cet argument, que le comité sectoriel approuve, qui justifie notre troisième réflexion.

C. La finalité affirmée

Le *testing* n'apparaît pas comme une finalité au sens de la loi de 1992, et en tout cas à supposer que oui, cette finalité n'est ni précise ni légitime. Par ailleurs en admettant même que cette finalité satisfasse à ces critères, la proportionnalité du contenu des données traitées n'apparaît pas respectée.

1. *Le testing* est-il une finalité et si oui cette finalité correspond-elle aux exigences de la loi du 8 décembre 1992 ?

Le comité sectoriel estime que le *testing* sur des données réelles et non simplement simulées, « comme s'il s'agissait d'une véritable transaction », est nécessaire pour que les tests soient efficaces et que « les applications puissent être corrigées et entretenues ». L'affirmation reprend littéralement la formulation de la demande de Fedict et on s'étonne que celle-ci soit peu étayée alors même que depuis des années le registre national, pour des raisons évidentes de sécurité, opère de tels tests sur des jeux de données simulées. Nous reviendrons sur cette question et les exceptions invoquées par Fedict qui justifient l'utilisation à titre exceptionnel de données réelles, lors de l'examen de la proportionnalité. La délibération estime que « c'est pour cette raison que le demandeur souhaite un accès aux informations ainsi qu'au numéro d'identification. Cela signifie que l'accès et l'utilisation souhaités seront exclusivement autorisés pour exécuter des tests internes et l'échange dans le cadre de tests de données avec des institutions qui disposent des autorisations nécessaires » et conclut dès lors que « la finalité poursuivie est déterminée, explicite et légitime au sens de l'article 4, § 1er, 2°, de la L.V.P. ».

L'affirmation ne cesse d'étonner. Tester n'est pas une finalité en soi et n'acquiert sa légitimité que par la légitimité des opérations à tester. La délibération détache la finalité de test de ces autres opérations pour en faire une base légitime à elle seule des opérations de Fedict, ainsi promu comme responsable de ce traitement à part entière. Le propos a de quoi étonner. Si une entreprise dans le cadre d'un contrat avec une entreprise ou de contrats multiples avec des entreprises fournit des services applicatifs de transport d'informations entre cette ou ces entreprises et doit tester la qualité de son service de transport, dira-t-on que celui-ci opère ce *testing* comme une mission propre. D'évidence, non. Il s'agit d'une opération qui s'intègre au service qu'il offre et qui en constitue un critère de qualité. « La Commission de la protection

[15] E. Degrave et Y. Poullet, *eod. loco.*

de la vie privée a eu l'occasion de préciser en quoi doit consister la finalité d'un traitement effectué dans le secteur public. Selon elle, l'objectif invoqué doit constituer une fin en soi et non un moyen »[16]. En d'autres termes, la finalité n'est pas le *testing* mais ce pour quoi le testing est nécessaire à savoir assurer les communications légitimes du registre national vers des administrations autorisées. C'est au regard de ces finalités qui légitiment la communication que le *testing* peut s'avérer indispensable comme moyen d'assurer la qualité et la sécurité des transmissions[17].

Par ailleurs, on connaît la jurisprudence de la Commission qui insiste sur le caractère strictement nécessaire des traitements opérés par l'administration publique et sur ce point on peut douter que les missions conférées à Fedict à savoir le « développement de projets et services qui englobent potentiellement l'ensemble des services publics fédéraux et qui soutiennent ces stratégies communes » (article 2, arrêté royal du 11 mai 2001) justifient la possibilité dans le cadre d'un *testing* d'applications développées par Fedict de pouvoir disposer d'un accès illimité au registre national. On rappelle le cas de l'a.s.b.l. nationale créée pour l'identification des chiens qui avait souhaité l'accès au registre national pour tenir un registre à jour des propriétaires de chiens, une telle demande a été rejetée dans la mesure où elle excédait les missions confiées à l'a.s.b.l.[18]

Ensuite, la finalité doit être déterminée et explicite, selon les exigences de la loi du 8 décembre 1992. Sans doute dira-t-on, la finalité est déterminée par référence à la nécessité de tester la qualité des communications entre le registre national et les autorités administratives autorisées à y accéder. Une telle finalité renvoie à une infinité d'autorisations et ne permet pas d'apprécier par rapport à un *testing* particulier à quelle autorisation il se rapporte.

En outre, « Le respect de l'exigence d'une finalité déterminée et explicite ne se satisfait pas d'une simple mention vague de l'objectif poursuivi par le traitement. Il importe que la finalité poursuivie soit déterminée avec précision. La Commission de la protection de la vie privée a avancé certains critères permettant de circonscrire une telle exigence de précision, rappelant à cette occasion que « la description des finalités poursuivies doit être aussi précise, détaillée et complète que possible »[19]. La raison

16 E. Degrave, « Examen de jurisprudence de la Commission de protection de la vie privée relative à la notion de finalité », article à paraître.

17 À cet égard on aurait pu souhaiter que le comité sectoriel réponde à l'objection du registre national. Fallait-il introduire le *testing* par un tiers en l'occurrence Fedict et ne pouvait-on se contenter du *testing* de la communication entre le registre national et l'instance destinataire et ne faire intervenir ce tiers que dans la mesure où la connexion posait difficulté, ce qui sans doute eût été exceptionnel ? La seconde solution présentait des avantages évidents dans la mesure où elle limitait au strict minimum l'intervention de Fedict et son besoin d'accéder à des données du registre national. Et dès lors paraissait plus conforme à l'exigence de proportionnalité des traitements qui implique le choix de la voie la moins attentatoire à la vie privée. Cette exigence du choix de la voie la moins attentatoire est rappelée par la Cour d'arbitrage. Dans l'affaire du décret de la Communauté flamande portant publication d'une liste noire de sportifs reconnus s'étant dopés, la Cour estime que « la publication entreprise n'est pas nécessaire pour atteindre l'objectif poursuivi par le législateur décrétal, puisque cet objectif peut également être réalisable par des moyens moins dommageables pour les intéressés » (C.A., arrêt n° 16/2005).

18 Sur cette décision et d'autres, lire de Bot, *op. cit.*, p. 167, n° 444. *Cfr* également la délibération n° 29/2004 du comité sectoriel registre national qui estime qu'une a.s.b.l. de promotion des femmes si elle poursuit une tâche d'intérêt général ne peut au nom de cette tâche justifier la communication par le registre national de femmes âgées de plus de 100 ans.

19 C.P.V.P., avis n° 02/2007 du 17 janvier 2007, relatif au projet d'arrêté royal déterminant les règles suivant lesquelles certaines données hospitalières doivent être communiquées au Ministre qui a la Santé publique dans ses attributions, § 13.

d'être de cette précision est évidente. Il s'agit de pouvoir apprécier aisément, d'une part, la proportionnalité tant du traitement : « la finalité décrite rend-t-elle nécessaire l'opération envisagée ? »[20] et, d'autre part, celle du contenu du traitement à savoir les données traitées et la durée du traitement, en d'autres termes d'éviter voire d'« d'exclure tout malentendu et toute discussion »[21] sur l'étendue des accès demandés et de pouvoir « apprécier facilement et valablement la pertinence et la proportionnalité des données collectées »[22].

2. *La proportionnalité du contenu du soi-disant traitement*

C'est ce point que nous examinons maintenant. De Bot[23] estime que la demande doit établir clairement le besoin exact (« de exacte behoefte ») de l'accès aux données et de l'utilisation du numéro de l'identification et sur cette base, la preuve de la proportionnalité des données réclamées et du numéro de registre national réclamé et finalement la fixation du délai de traitement de telles données. Sur ces trois points on hésite à suivre le raisonnement du comité sectoriel. Quatre objections peuvent selon nous être adressées au raisonnement du comité.

Premièrement, il est établi que la qualité de la connexion avec le registre national n'impliquait pas nécessairement l'utilisation de données réelles. La demande distingue trois cas où cette utilisation est nécessaire : « pour l'établissement et le test de la connexion finale qui sera utilisé en production lors de la mise en place d'une première connexion avec un nouveau service ou lors de la mise en production d'une nouvelle version ; lorsque des divergences semblent apparaître entre l'environnement test et l'environnement de production,... ; lorsque la réaction de l'environnement de production est différente des prévisions ou des spécifications ». En d'autres termes, le besoin décrit par la demande de Fedict ne fait pas apparaître, loin de là, la nécessité d'un accès permanent aux données réelles du registre national et plaide pour un accès subsidiaire limité au cas où l'exigent les expériences menées sur des données test par le registre national et l'autorité qui a obtenu l'accès au registre[24]. Certes, ce besoin peut se révéler à divers moments ainsi lors du démarrage d'un nouveau service proposé par Fedict ou lors d'une release de ce service ou d'une application liée à ce service mais on est loin de pouvoir justifier un accès permanent.

Deuxièmement, alors même que la demande ne précisait pas les données du registre national[25] auxquelles Fedict souhaitait avoir accès, « le comité déduit de celle-ci que le demandeur souhaite un accès aux informations mention-

20 Dans la mesure où la finalité constitue le cadre dans lequel les données peuvent être traitées (C.P.V.P., avis n° 01/2007 du 17 janvier 2007, *op. cit.*, § 10).

21 C.P.V.P., avis n° 13/2004 du 21 octobre 2004, relatif au projet d'arrêté royal déterminant les personnes et institutions ayant accès au registre des cartes d'identité, § 3.1.1.

22 C.P.V.P., avis n° 14/2006 du 24 mai 2006, relatif au projet d'arrêté royal déterminant les règles suivant lesquelles certaines données hospitalières doivent être communiquées au Ministre qui a la Santé publique dans ses attributions, § 27. En ce sens, également les conclusions de E. Degrave dans l'examen de jurisprudence déjà cité.

23 De Bot, *op. cit.*, pp. 169 et s.

24 À cet égard la description du cas de la demande d'accès par la Chambre des représentants d'un accès permanent au registre national pour vérifier l'égibilité des représentants du peuple alors que les élections ou les suppléances ont lieu à des moments précis (délibération du comité sectoriel n° 06/2004 du 15 mars 2004) et dans le cadre d'une demande de vérification régulière pour la mise à jour de fichiers tenus par le Regionale Milieuzorg et la s.a. Cegeka, la limitation à un accès une fois par an (délibération du comité n° 17/2004 du 14 juin 2004), voy. également dans la jurisprudence du comité sectoriel « autorité fédérale », les délibérations (n^{os} 01/2005 ; 06/2007 et 01/2007).

25 Comme relevé par le comité sectoriel lui-même : « Bien que cela ne soit pas expressément formulé mot pour mot dans la demande... ».

nées à l'article 3, premier et deuxième alinéas de la loi sur le registre national ». Ainsi, alors même qu'aucune preuve de proportionnalité n'est apportée, le comité sectoriel octroie un accès à la fois à l'ensemble des données de base mais également à l'historique de telles données, dont pourtant la Commission s'accorde à reconnaître un caractère plus sensible[26]. On connaît la prudence traditionnelle du comité, relevée par de nombreux auteurs, lorsqu'il s'agit de déterminer l'ampleur de l'accès au registre national. « Les données doivent être limitées à ce qui est nécessaire, adéquat et pertinent à la réalisation de la finalité poursuivie. La loi exige également des conditions de qualité concernant les données à caractère personnel faisant l'objet d'un traitement. L'article 4, § 1er, 3°, de la loi sur la vie privée prévoit que les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement »[27]. Cette prudence contraste avec la largesse dont fait preuve cette fois le comité sectoriel en statuant *ultra petita*. S'il s'agit de tester des connexions autorisées avec le registre national, le test ne doit-il pas être limité aux seules données auxquelles l'accès a été autorisé dans le cadre de la connexion testée. Ainsi, si par hypothèse, seules cinq données de base peuvent faire l'objet d'un accès par telle autorité, on ne conçoit pas que l'accès soit étendu à l'ensemble des données y compris de leur historique. Il va de soi qu'un tel accès non sélectif en fonction des autorisations de communications auxquelles le test s'applique crée un risque non négligeable de détournement de finalités et en tout cas interdit au registre national de pouvoir vérifier si la demande est adéquate au regard de l'autorisation accordée. Nous reviendrons dans le point 4 sur cette question délicate.

Le comité sectoriel introduit cependant au nom de la proportionnalité deux limites dont on cherche vainement à comprendre le caractère adéquat. Ainsi, la délibération affirme qu'« un accès illimité n'est pas justifié, tant du point de vue de la sécurité que de la proportionnalité... ». Il fixe dès lors, « les conditions et restrictions suivantes :... le conseiller en sécurité du demandeur (Fedict) détermine la population qui peut faire l'objet des tests ; cette population comprend un maximum de 10 000 personnes et le conseiller en sécurité contrôle scrupuleusement le respect de ces paramètres... ». Ainsi, on note qu'on voit mal sur quelles bases la population sera déterminée[28] ; quant au choix du chiffre de 10 000 personnes, il n'est aucunement justifié et pourra apparaître *in casu* comme démesuré.

Troisièmement, le comité propose que l'accès soit permanent et à durée indéterminée, étant donné que, selon le comité, « la finalité exige que le demandeur soit en mesure de procéder à tout moment aux tests d'une application, à son contrôle ou à son entretien... » et que « les phases de test, de correction et d'entretien font essentiellement partie de la gestion de projet et de service de projets d'e-government ». La permanence est justifiée par une « exécution correcte » des tâches de Fedict. À nouveau, il eût été intéressant de nuancer le propos et sur la base de l'exigence de proportionnalité de prévoir des droits d'accès liés à des opérations précises lors du lancement de nouvelles appli-

[26] *Cfr* en particulier, l'avis n° 19/2002 à propos du projet de loi de révision de la loi de 1983 sur le registre national.

[27] Comité sectoriel de l'autorité fédérale, n° 04/2007, point 26 ; *cfr* surtout les décisions du comité sectoriel relatives aux demandes de la Commission bancaire, financière et des assurances n° 33/2004 du 25 novembre 2004 et n° 12/2004 du 26 avril 2004.

[28] Sauf à considérer que cette population sera sélectionnée au cas par cas en fonction des différentes autorisations données par le comité sectoriel.

cations et, selon une régularité à justifier, pour des opérations de contrôle.

Quatrièmement à propos de la durée de conservation, le comité sectoriel analyse d'abord la durée de conservation des données des résultats des tests : les données relatives à X ont bien été testées dans le cadre d'une communication entre le registre national et telle instance ou institution déterminée et en faisant usage de l'application ou du service A. La demande distingue à leur égard deux hypothèses : le test est réussi et les données testées doivent être effacées. La solution est heureuse ; encore faut-il savoir ce que l'on entend par test réussi, qui décide de la réussite et les méthodes de contrôle de la destruction des données, ce que la demande ne précise pas et qui pourtant apparaît comme une garantie minimale d'effectivité de l'engagement pris par Fedict. Dans le second cas (test non réussi), la durée de conservation d'un an maximum est proposée et acceptée par le comité sectoriel. Cette durée apparaît peu justifiée.

La durée de conservation des logs des activités de test (Qui a accédé ? À quoi a-t-il accédé ? Quand a-t-il accédé ?) est fixée, quant à elle, à 10 ans par l'autorisation du comité. La finalité d'une telle conservation est différente certes. Il s'agit de détecter d'éventuels accès illégitimes aux données testées et ainsi des détournements de finalité. Peu d'objections à une telle durée, même si on eût souhaité que référence à la durée de conservation des logs dans d'autres administrations soit faite.

En conclusion, peu de limites sont mises par le comité sectoriel à l'accès aux données du registre national et à l'utilisation du numéro d'identification national, ni dans les données auxquelles l'accès est donné, ni quant à la durée de cet accès et de cette utilisation. Cette absence de limites soulève des difficultés pour le registre national dans la mesure où il est responsable de la sécurité des traitements qu'il opère, à savoir ceux relatifs à la source authentique que constitue le registre national. Cette difficulté est encore aggravée par le fait que le comité sectoriel lui impose d'accepter un système de connexion avec Fedict fondé sur un simple certificat d'application. La généralisation de ce système prônée par le comité sectoriel met à mal non seulement l'obligation de sécurité imposée au registre national comme responsable de traitement mais au-delà la transparence des flux de données à partir du registre national imposée par le législateur. Ceci constitue le dernier point de notre réflexion.

D. La connexion de Fedict au registre national

La connexion de Fedict au registre national par l'utilisation d'un simple certificat d'application constitue une remise en cause de l'obligation de sécurité à charge du registre national comme responsable de traitement et de l'obligation de transparence vis-à-vis du citoyen des flux opérés par le registre national.

La proposition est double. D'une part, nous préoccupe la difficulté pour le registre national d'accomplir l'obligation de sécurité qui incombe au registre national sur la base de l'article 16 de la loi du 8 décembre 1992. D'autre part, la décision met en cause les devoirs de transparence que le législateur a imposés au registre national au bénéfice des citoyens.

1. La remise en cause de l'obligation de sécurité

L'autorisation du comité sectoriel consacre une large part de ses développements à une description des mesures de sécurité que Fedict s'apprête à mettre en place dans le cadre du développement des protocoles U.M.E. et F.S.B. Comme déjà signalé lors de l'analyse du premier argument, cette description atteste

du véritable enjeu de la demande de Fedict de devenir à moyen terme à l'instar de la B.C.S.S. un véritable intégrateur de services de transport sécurisé disposant de bases de données de référence. Cette décision n'est pas en soi critiquable mais devrait être l'objet d'une discussion législative et non d'une mise en place progressive et larvée. Ces mesures de sécurité concernent l'authentification des utilisateurs et des serveurs des protocoles U.M.E., des services web et du F.S.B. et la constitution d'un *audit trail*[29]. Il est évident que ces mesures vont bien au-delà des applications de test analysées dans le cadre de la délibération analysée.

Leur description est approuvée ou plutôt « recommandée » par le comité sectoriel dans la mesure où il permet d'appuyer la politique des « cercles de confiance » mise en place par Fedict dans le cadre de ses devoirs de sécurité. Ces mesures de sécurité sont telles que le comité estime « que les applications du demandeur doivent être uniquement authentifiées vis-à-vis du registre national par un certificat d'application » et non plus comme c'est le cas actuellement pour les connexions au registre national par la communication du moyen d'identification et d'autorisation. Ceci, poursuit le comité, « évite que soit constituée au sein du registre national une banque de données dont le registre national n'a pas besoin pour l'exécution de ses missions », à savoir la liste des personnes autorisées à accéder au registre national et le log de toutes les demandes individualisées de connexion au registre national.

Or, la constitution de telles banques de données constitue indiscutablement une des mesures de sécurité prises par le registre national conformément à ses obligations de sécurité, obligations auxquelles sont tenus les responsables de traitement, en l'occurrence le registre national. Elles permettent au registre national notamment de s'assurer que seules les personnes autorisées dans les diverses institutions admises à accéder au registre national ont accès à ce dernier, de vérifier qu'elles n'outrepassent pas leur habilitation et, au-delà de cet accès, de conserver une trace de celui-ci à des fins de preuve. Le comité va plus loin puisqu'il estime que les mesures de sécurité prises par le registre national constituent un risque d'atteinte à la vie privée des utilisateurs dans la mesure où l'enregistrement systématique de leur demande de connexion crée à leur endroit une suspicion. « De telles conséquences malheureuses ne se produiraient pas si le registre national n'enregistrait pas les utilisateurs individuels comme cela a été recommandé par la Commission le 8 février 2006 ».

La conservation des logs est un élément important de la politique de sécurité. La Commission belge de protection de la vie privée encourage de tels mécanismes de journalisation et de traçage, qui doivent permettre de retrouver en cas de nécessité, d'accès non autorisé ou abusif ou de manipulation des données, l'identité de l'auteur[30]. La même obligation se retrouve au niveau européen. Le règlement 45/2001[31] prévoit en son article 22 : « Lorsque des données à caractère personnel font l'objet d'un traitement automatisé, des mesures sont

29 « Un *audit trail* est un fichier qui contient toutes les données significatives qui fournissent une preuve qu'une transaction ou un événement spécifique s'est déroulé à un moment précis », F. Coppens, « *Audit trail* : protection des données et e-gouvernement à travers la question des logs », mémoire D.T.I.C., avril 2008, p. 16.

30 C.P.V.P., « Mesures de référence en matière de sécurité applicable à tout traitement de données à caractère personnel », document SE/05/048, p. 3, disponible sur le site de la Commission.

31 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

prises lorsqu'elles sont nécessaires au regard des risques encourus, notamment dans le but : ... (f) de garder une trace des données à caractère personnel qui ont été communiquées, du moment où elles l'ont été et de leur destinataire ; (g) de garantir qu'il sera possible de vérifier *a posteriori* quelles données à caractère personnel ont été traitées, à quel moment et par quelles personnes ». Il va de soi que vis-à-vis d'une base de données dont l'utilisation est aussi génératrice de risques que le registre national, de telles mesures de sécurité doivent être prises par le responsable du traitement et la pratique du registre national qui demande à chaque autorité de désigner fonctionnellement les personnes autorisées et leur niveau d'autorisation est depuis longtemps consacrée par les décisions de la Commission, des comités sectoriels, ensuite.

Sans doute, peut-on admettre que la conservation des logs est elle-même génératrice de risques dans la mesure où cette conservation constitue un traitement qui permet de détecter par utilisateur les accès effectués, ce qui peut dans certains cas attenter au secret professionnel ou simplement au devoir de discrétion des utilisateurs du registre national. Ainsi, il permettrait de savoir que tel notaire ou tel avocat fait des recherches sur telle personne et laisse induire une relation entre cet avocat et cette personne. C'est pourquoi, au nom de la balance d'intérêts, on peut concevoir que dans le cadre de certaines professions ou pour certains services (ex : la sûreté de l'état ou la police), les utilisateurs puissent passer par un Trusted Third Party (T.T.P.) de la profession ou de l'administration et que l'accès puisse se réaliser par le certificat d'application du T.T.P. C'est notamment ce souhait que formule la fédération des notaires[32] qui se propose comme T.T.P. Dans de tels cas exceptionnels, l'utilisation d'un certificat d'application peut être envisagée, moyennant des précautions comme l'obligation du T.T.P., de révéler le demandeur final d'accès au cas où une plainte est formulée vis-à-vis du registre national pour un accès abusif ou non autorisé. Bref, un log des demandeurs d'accès est alors tenu par le T.T.P.

Dans le cas de Fedict, on voit mal les raisons qui pourraient plaider en faveur d'une telle procédure. On le voit d'autant plus mal que l'étendue de l'accès est mal précisée (voy. *supra* C, point 2) et que l'accès par le certificat d'application de Fedict sera possible non seulement pour Fedict mais également ses sous-traitants non désignés et qu'aucune garantie n'est donnée sur la façon dont les logs seront tenus et mis à disposition du registre national en cas de problèmes, etc[33]. Il est clair en tout cas que la sécurité des traitements engendrés par le fonctionnement du registre national incombe à ce dernier en tant que responsable de cette source authentique et ne peut être mise en cause à l'occasion de ce qui apparaît un blanc-seing vis-à-vis de Fedict et de ses sous-traitants. On regrette que le comité sectoriel se soit contenté de stigmatiser les risques mineurs

[32] À cet égard, le mémoire de Fr. Coppens déjà cité (pp. 21 et 22, en particulier), qui propose un système d'*audit trail* où chaque membre de la chaîne (le notaire, le Credoc services agissant comme sous-traitant de la Fédération et le registre national) aurait une responsabilité dans l'enregistrement des traces de manière à garantir par une approche décentralisée la sécurité des accès aux données du registre national.

[33] À noter que très récemment, dans son avis n° 23/2008 du 11 juin 2008 (objet : avant-projet de loi portant création de la source authentique des données relatives aux véhicules), la Commission de protection de la vie privée plaide pour un enregistrement centralisé de logging même si elle reconnaît la possibilité de l'alternative des enregistrements décentralisés. « Un enregistrement centralisé de logging au niveau de responsable du traitement, à savoir la D.I.V., semble offrir plus de garanties. Cette méthode semble permettre plus facilement un contrôle indépendant de l'utilisation des données, au lieu de l'enregistrement local de telles données qui peut se révéler plus difficilement contrôlable... ».

relatifs à la création par le registre national et à l'occasion de la demande très particulière de Fedict de condamner de manière générale le système de logs tenus par le registre national, système qui est pourtant essentiel à la sécurité des traitements opérés par ce dernier. La « recommandation » du comité sectoriel à l'encontre du système actuel du log des numéros d'identification et d'authentification des utilisateurs du registre national est d'autant plus regrettable que ces logs permettent au registre national de remplir une obligation légale qui contribue à la confiance et à la transparence de son fonctionnement. C'est le second point que nous évoquons.

2. Les obligations réglementaires de transparence du registre national

Qu'on le fonde sur l'article 32 de la Constitution qui consacre le droit à l'information du citoyen vis-à-vis des autorités publiques ou sur le droit d'accès consacré par l'article 10 de la loi de 1992 qui accorde le droit d'accès aux personnes concernées, le devoir de transparence des administrations vis-à-vis des personnes concernées est un principe fondamental de l'action administrative. En ce qui concerne le registre national, le législateur l'a consacré d'une manière particulière, eu égard aux craintes d'abus ou aux risques d'erreur, que le fonctionnement de cette source authentique peut engendrer. Dans ce contexte, l'article 6, § 3, second alinéa de la loi du 19 juillet 1991 relative aux registres de population, aux cartes d'identité et aux documents de séjour, et modifiant la loi du 8 août 1983 organisant un registre national des personnes physiques (*M.B.*, 3 septembre 1991), prescrit que « le titulaire d'une carte (d'identité) a le droit de demander, au moyen de cette carte ou auprès de la commune dans laquelle il est inscrit aux registres de la population : ... 3° de connaître toutes les autorités, organismes et personnes qui ont, au cours des six mois écoulés, consultés ou mis à jour ses données au registre de la population ou au registre national des personnes physiques, à l'exception des autorités administratives ou judiciaires, chargées de la recherche et de la répression... ».

L'imposition de cartes d'identité électronique a amené le gouvernement à prévoir que celles-ci puissent également servir afin de rendre plus effectif ce droit d'accès à l'information. L'arrêté royal du 5 juin 2004 prescrit que chaque porteur d'une carte d'identité électronique dont le mécanisme d'authentification et de signature est activé doit avoir accès y compris à distance et ce par le biais d'un lecteur de carte approprié à l'ensemble des informations prescrites par l'article 6, § 3, 2e alinéa, 3°, précité [34].

Cette mesure légale complétée par la disposition de l'arrêté royal[35] permet à tout citoyen moyennant son authentification à distance par sa carte d'identité électronique et l'introduction de son numéro secret de pouvoir connaître les utilisateurs ayant eu accès aux données le concernant figurant au registre national, comme le note D. De Bot[36].

Bien que limitée pour l'instant au registre national, la consécration d'un droit d'accès à distance apparaît comme une amélioration nécessaire de la transparence des flux au moment où le gouvernement électro-

[34] Sur cet arrêté royal, lire De Bot, *op. cit.*, p. 222.

[35] Cette disposition a été mise en vigueur suite à l'arrêté royal du 13 février 2005 déterminant la date d'entrée en vigueur et le régime du droit de prendre connaissance des autorités, organismes et personnes qui ont consulté et mis à jour les informations reprises dans le registre de population ou au registre national des personnes physiques (*M.B.*, 28 février 2005). L'arrêté précise que le droit s'exerce « au moyen d'un appareil de lecture relié à un ordinateur connecté à Internet et par l'intermédiaire du site internet du registre national ».

[36] D. De Bot, *Privacybescherming bij e-government in België*, Van den Broele, 2005, p. 216, note 576.

nique multiplie ceux-ci et se dote d'outils de plus en plus performants de communication de données[37]. Elle entend maintenir ainsi la confiance du citoyen dans le fonctionnement de l'administration. On s'inquiète dès lors du revirement que constitue la délibération du comité sectoriel visé. Les raisons invoquées pour exempter légalement de cette transparence les services de police, de renseignements et de sûreté sont loin de se retrouver dans le cas de Fedict. L'utilisation d'un certificat d'application a pourtant pour effet de rendre opaque les multiples demandes d'accès que Fedict et ses sous-traitants pourraient opérer auprès du registre national à des « fins » de *testing* et de permettre le contrôle par les citoyens de l'ampleur de ceux-ci et d'empêcher le citoyen d'interroger les agents dont le nom apparaît sur la liste des personnes ayant eu accès au registre national sur les raisons de cet accès et de détecter ainsi les abus possibles ou les consultations anormales.

Le point de vue du comité sectoriel contredit la loi de 1991. Il est difficile de plaider que la notion de « personnes » utilisée par la loi ne vise pas les personnes physiques, c'est-à-dire les fonctionnaires ou mandataires ayant consulté ou modifié les données du registre national. L'argument de protection de la vie privée de ces fonctionnaires ou mandataires qu'avance le comité sectoriel est peu tenable. Si le registre national et la personne concernée peuvent par le biais de ce droit d'accès connaître le nom de ceux qui ont accédé à ses données, c'est au nom de l'intérêt supérieur de la personne concernée que traduit le droit d'accès consacré par le législateur et de l'obligation de sécurité qui existe dans le chef du registre national comme responsable du traitement. Ce dernier a d'ailleurs pris soin d'exempter de cette transparence les agents de certains services nommément cités comme les « autorités administratives et judiciaires chargées de la recherche et de la répression ». *A contrario*, il semble difficile d'admettre toute autre exception même si certaines pourraient être concevables lorsque l'accès au registre national se justifie par l'exécution d'une mission dont la confidentialité doit être assurée au nom de valeurs supérieures à celles qui justifient le droit d'accès de la personne concernée.

Ce raisonnement limitant strictement l'exception amène à s'interroger sur la légalité de la pratique qui a lieu en cas d'interrogation du registre national via la Banque-carrefour de sécurité sociale. Les « fichiers logs » de connexion des serveurs de cette organisation agissant comme organisation intermédiaire sont en effet conservés par la Banque-carrefour et non transmis au registre national. Une telle pratique n'est valable à notre sens que si cette conservation à l'extérieur du registre national ne rend pas plus difficile la consultation par le citoyen porteur d'une carte des données relatives aux utilisateurs du registre national, qui se sont connectés via la Banque-carrefour de sécurité sociale.

[37] Le droit à un accès à distance du citoyen à ses propres données à caractère personnel constitue une application de ce que nous avons appelé le principe de « réciprocité des avantages ». « La justification du principe est simple, si la technologie accroît les capacités de collecte de traitement, de communication des informations relatives à autrui, si la technologie facilite la conclusion de transactions ou d'opérations administratives, il est indispensable que cette même technologie soit configurée et utilisée de manière telle que la personne concernée, l'administré, le consommateur, bref le fiché, puisse bénéficier, dans une proportion comparable, des avantages de cette technologie. Quelques dispositions récentes se fondent sur l'exigence de la réciprocité des avantages pour obliger celui qui utilise des technologies à mettre à disposition de l'internaute des moyens électroniques pour faire valoir ses intérêts ou ses droits qui peuvent être mis à mal par l'utilisation de ces moyens électroniques » (sur ce principe et d'autres exemples tirés des législations récentes en matière de protection des données, Y. Poullet, « La protection des données : un nouveau droit constitutionnel – Pour une troisième génération de réglementation de protection des données », *in Droit constitutionnel et vie privée,* Recueil des cours n° 17, Académie de droit international, Tunis, vol. XVII, p. 347, n° 52).

CONCLUSIONS

Les comités sectoriels, création de la loi de 2003, se mettent en place progressivement. Les avantages du système sont connus : la composition paritaire des comités permet une meilleure spécialisation voire expertise des membres, une meilleure connaissance des besoins de l'administration et surtout un contrôle plus effectif des flux en question. L'intervention *a priori* de ces comités permet une meilleure protection des citoyens.

On relèvera avec D. De Bot[38] qu'il est cependant à craindre que la proximité du terrain renforcée par le fait que chaque comité est « flanqué » d'une institution de gestion du secteur concerné, qui prépare l'avis technique et juridique relatif au dossier introduit par cette dernière[39], favorise en définitive une plus grande complicité avec les administrations chargées par ailleurs d'instruire le dossier[40].

La décision annotée illustre ces craintes et amène à s'interroger sur le contrôle du travail de ces comités. Sans doute, l'évocation par la Commission existe et peut s'opérer à la demande des présidents de la Commission ou du comité sectoriel lui-même. Au-delà, survient la délicate question du contrôle externe que pourrait jouer le Conseil d'État ou les juridictions ordinaires. Dans l'article qu'elle a publié dans cette revue en 2006[41], Mme Degrave s'interrogeait : « La Commission de protection de la vie privée : un organisme invincible ? » et analysait pour ce faire le statut de cette Commission et des comités créés en son sein. Après avoir rejeté la qualification tant d'organe du Parlement que d'autorité administrative, elle concluait : « Faut-il définitivement se résigner à considérer que la Commission est invincible ? Certainement pas. Une telle situation est inadmissible dans un État de droit » et envisageait dès lors des solutions tendant à la compétence du Conseil d'État qui « présenterait une incontestable cohérence par rapport aux attributions qui sont d'ores et déjà confiées à la juridiction administrative »[42].

On ajoutera à ce propos que la mise en place de cette solution de recours contre les décisions des comités n'est pas seulement un souhait mais constitue une obligation. L'article 28, § 3, alinéa 2, de la directive 95/46/CE du 24 octobre 1995, que notre législateur a transposé en 1998, énonce en effet : « Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel ». Reste à écrire cette page manquante qui met la Belgique en défaut d'honorer ses obligations européennes ou à forcer dès maintenant les autorités juridictionnelles à se déclarer compétentes et ainsi se mettre au service de nos libertés.

38 D. De Bot, « De Commissie voor de bescherming van de persoonlijke levensfeer : tussen droom en daad bestaaan er niet alleen wetten in de weg, maar vooral praktische problemen », *R.G.D.C.*, 2003, pp. 384 et s. *Cfr* également nos réflexions critiques *in* Y. Poullet, « L'autorité de contrôle : vues de Bruxelles », *Revue française d'administration publique*, n° spécial, 1999, pp. 69 et s.

39 *Cfr* article 31*bis*, § 3, de la loi du 8 décembre 1992, introduit par l'article 6 de la loi du 26 février 2003 (*M.B.*, 26 juin 2003).

40 Par ailleurs, la multiplication des comités sectoriels peut amener, outre une dilution des responsabilités, une diversité des jurisprudences. On ajoutera que la multiplication des flux entre administrations relevant de comités sectoriels distincts entraînera de délicats problèmes de partage des compétences entre les différents comités sectoriels. Enfin, il n'est pas évident qu'une vue globale et la définition de principes généraux valables pour l'ensemble de l'administration publique soient encore possibles.

41 *R.D.T.I.*, n° 25/2006, p. 225.

42 E. Maron cité par E. Degrave, article cité, p. 240.